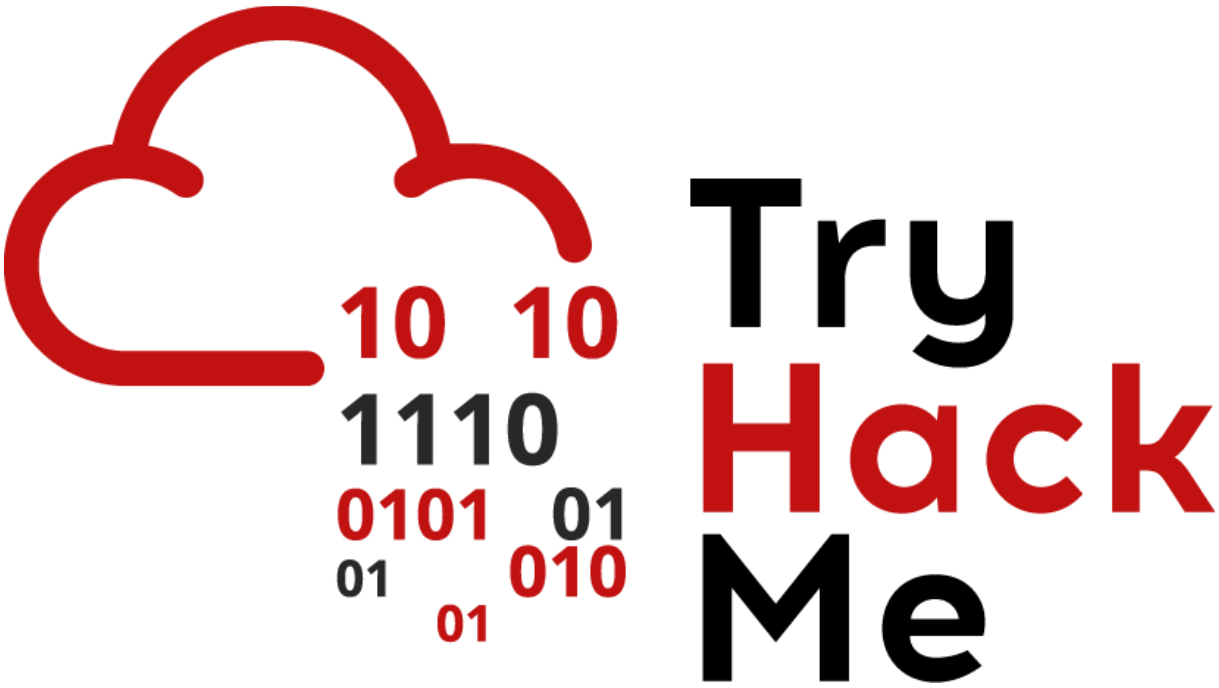


Document technique sur une room TryHackMe

Par

Grégoire LE BARON

Table des matières :

1- Introduction

TryHackMe est un site en ligne proposant des « rooms » qui permettent d'en apprendre plus sur la cybersécurité.

L'objectif de ce TP est d'analyser les trames Ethernet pour comprendre quelles sont les informations que nous sommes capables de reconstituer.

2- Prérequis

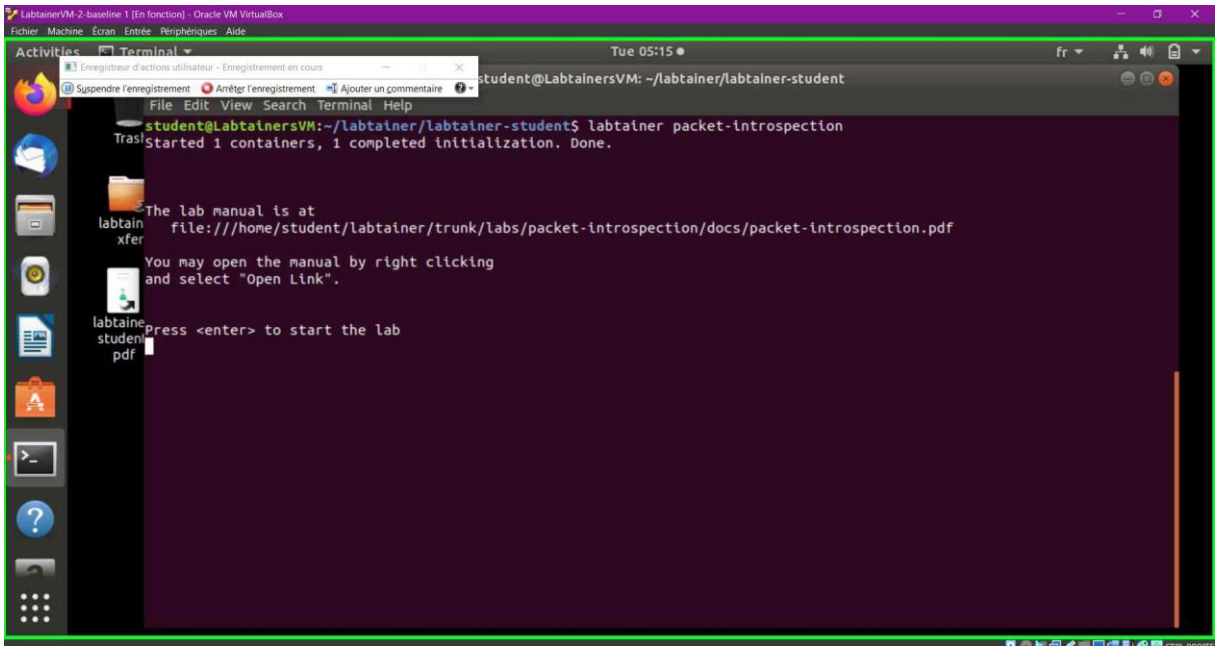
Pour réaliser cet atelier, il est nécessaire d'avoir un compte TryHackMe.

Le site met également à disposition une machine virtuelle en ligne pour s'exercer. Mais il est recommandé d'utilise sa propre machine virtuelle et de se connecter sur un VPN. Pour cela, il sera nécessaire d'avoir une machine virtuelle reposant sur le noyau Linux. Concernant la création d'une MV, vous pourrez retrouver la documentation technique.

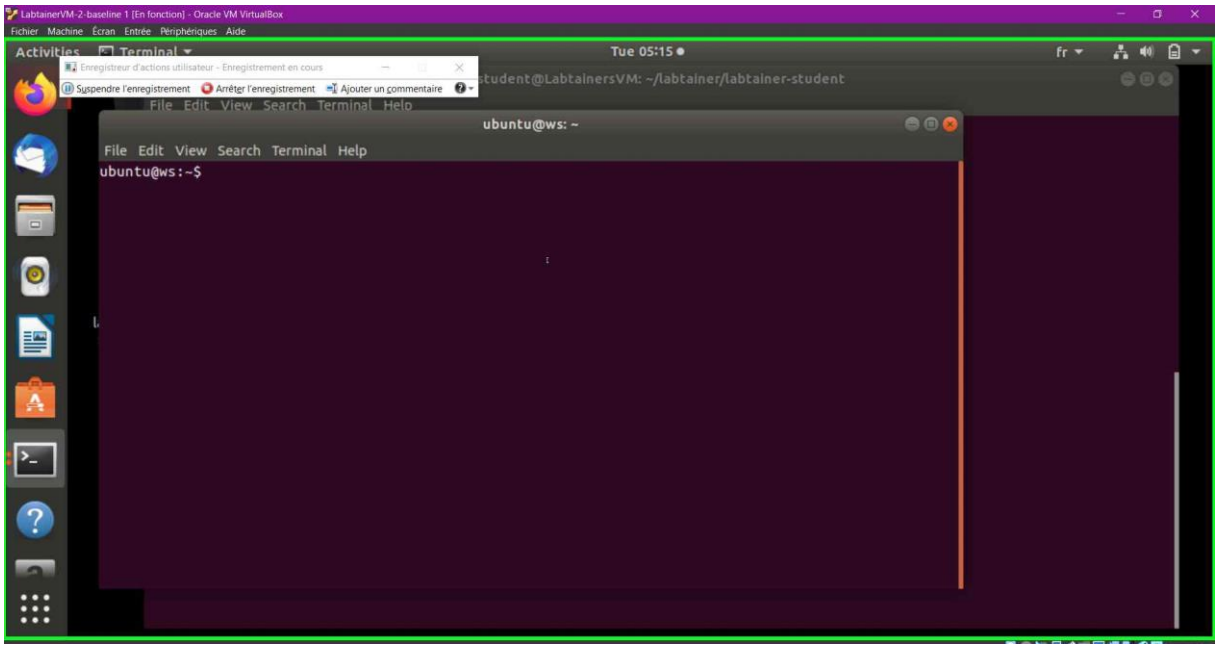
3- L'activité

a. Démarrer la session

Pour commencer, nous démarrons la machine virtuelle LabtainerVM. Ensuite, nous exécutons la commande « labtainer packet-introspection ».



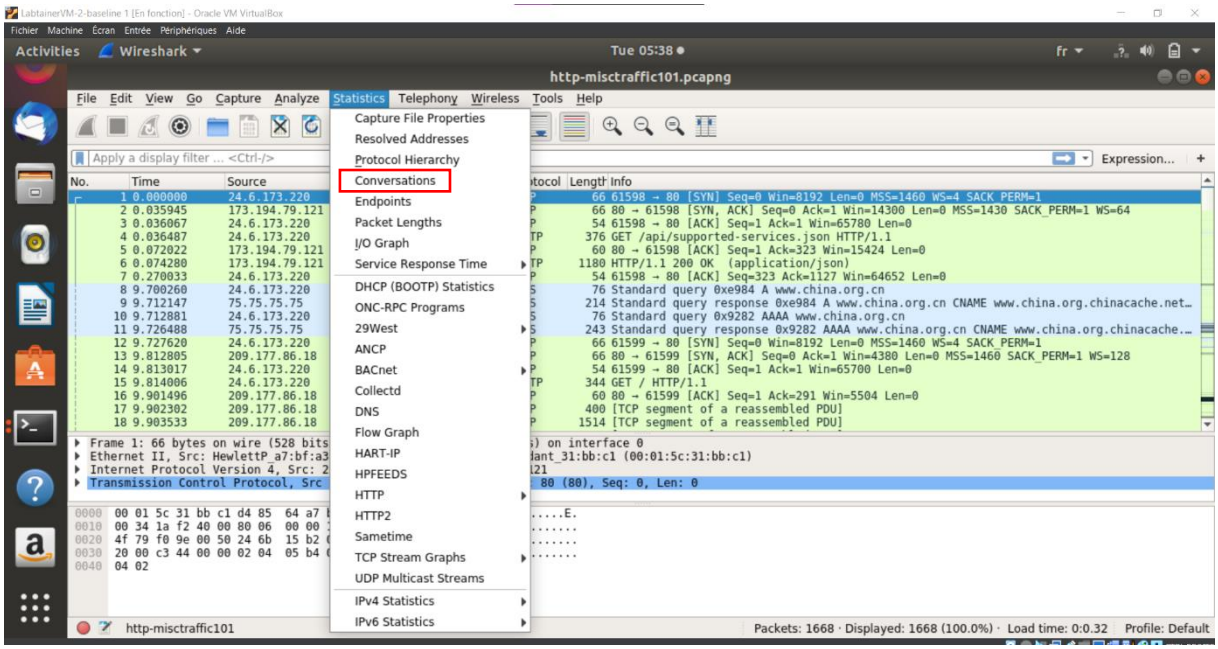
Cette commande permet d'ouvrir un nouveau terminal appelé « ws » et qui est connecté à un ordinateur client.



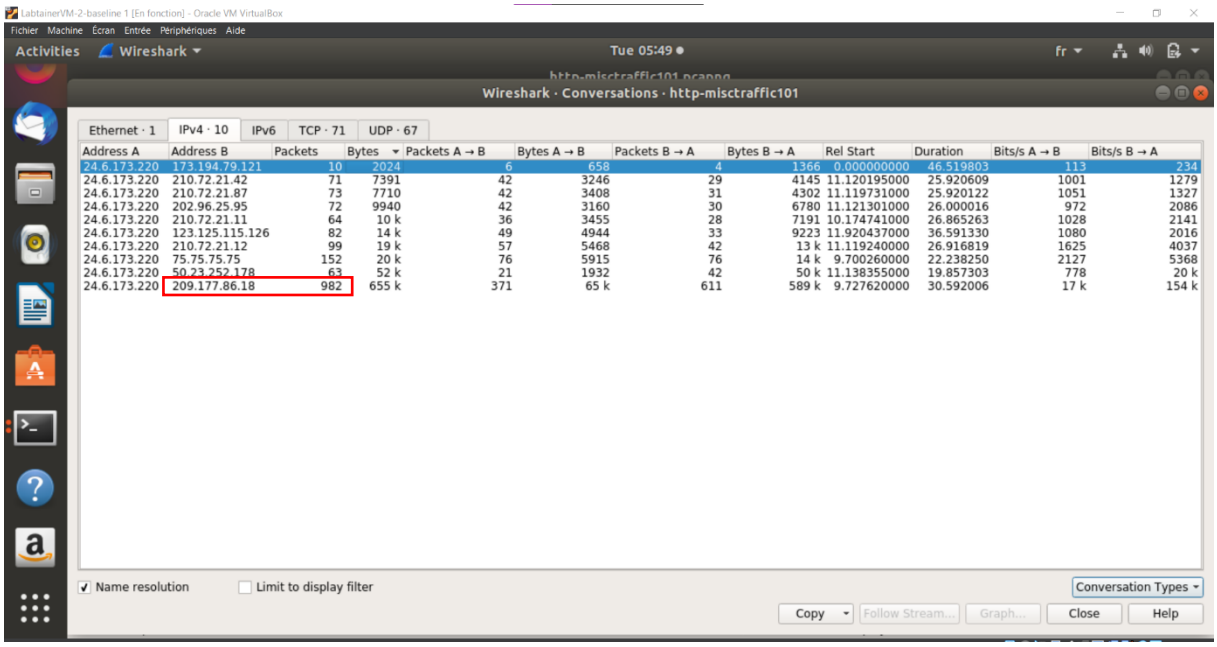
Dans ce terminal nous ouvrons wireshark en écrivant « wireshark ».

b. Trouver le flux TCP le plus actif

Nous ouvrons le premier fichier « pcaps/http-misctraffic101.pcapng ». Puis nous sélectionnons le paramètre conversations dans l'onglet statistics.



Cela ouvre une nouvelle fenêtre qui répertorie les échanges en fonction des adresses IP et des protocoles utilisés.

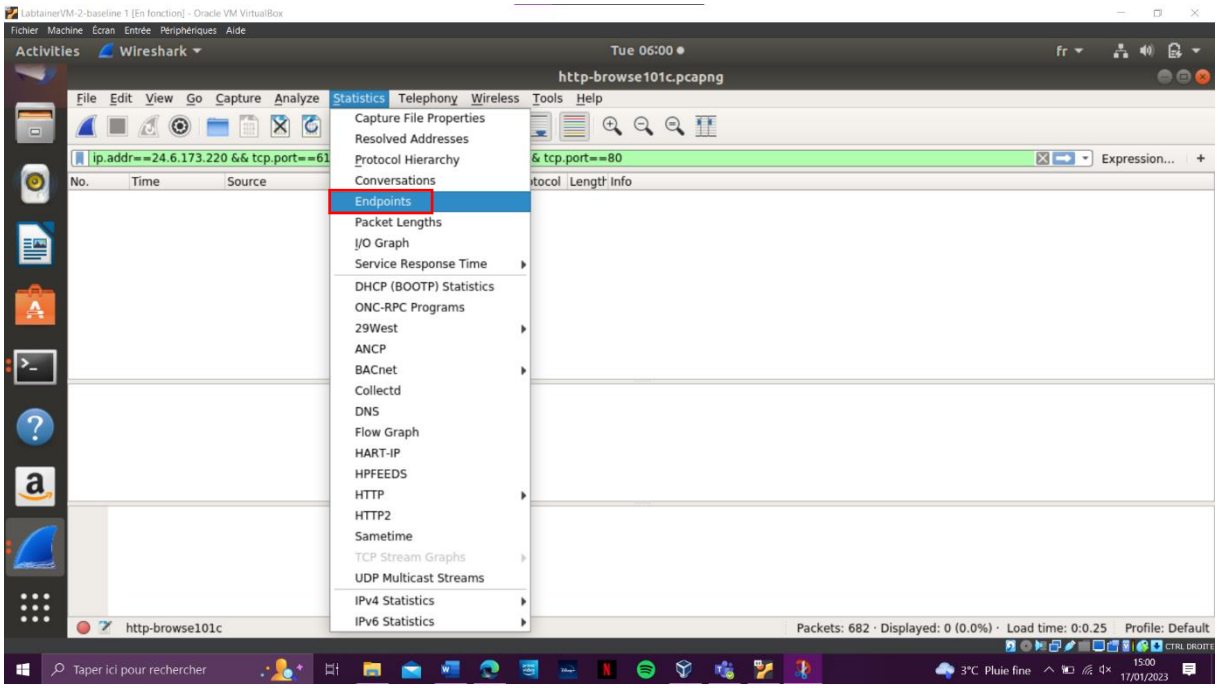


Nous observons que l'adresse IP24.6.173.220 a échangé 982 paquets, contenant au total de 655 k bits, avec l'adresse IP 209.177.86.18.

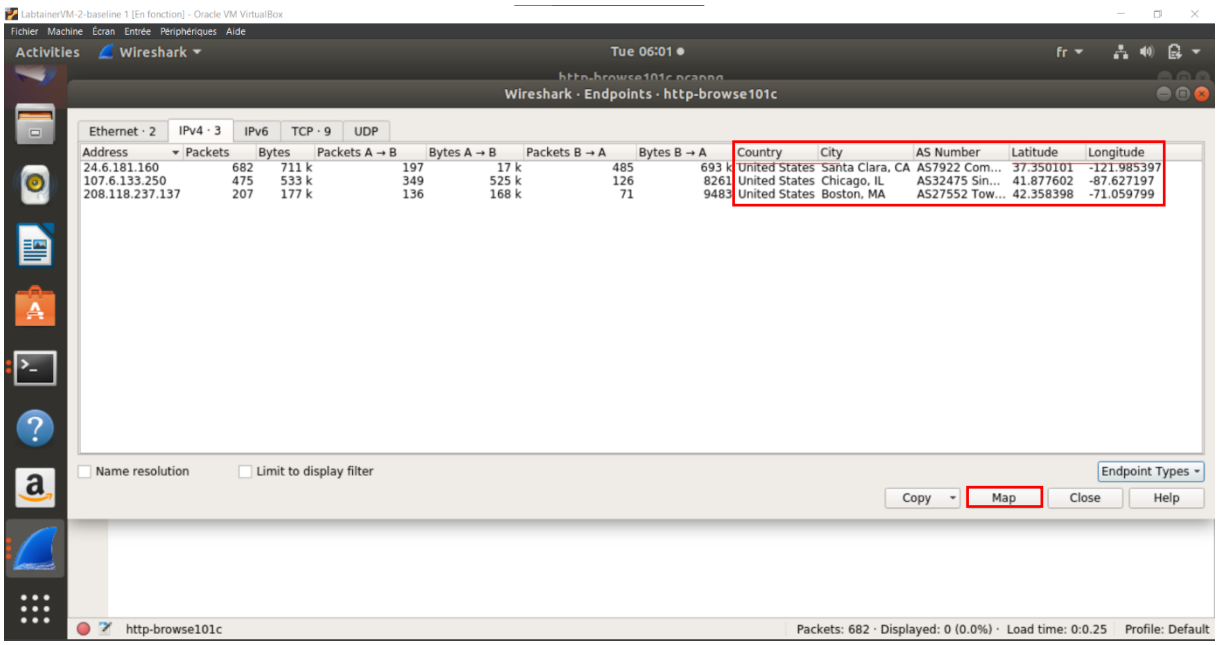
c. Géolocaliser des Adresses IP

Nous allons maintenant voir que nous sommes capables de localiser les différents serveurs avec lesquelles le client communique.

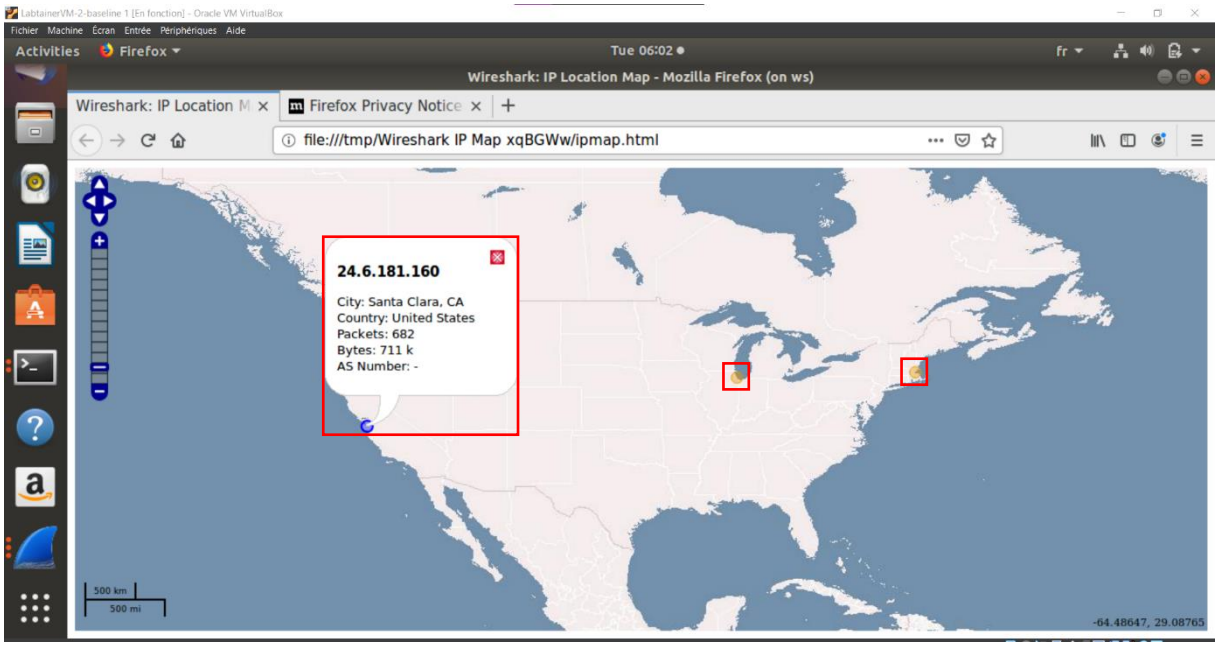
Nous ouvrons maintenant le fichier « pcaps/http-browse101c.pcapng ». Nous sélectionnons également le paramètre Endpoints dans l'onglet statistics.



Nous obtenons la page suivante :



Nous observons que nous avons des informations sur la localisation de chaque adresses IP. Nous cliquons sur le bouton « Map » pour visualiser ces informations sur une carte. Nous obtenons la vue cartographique suivante :

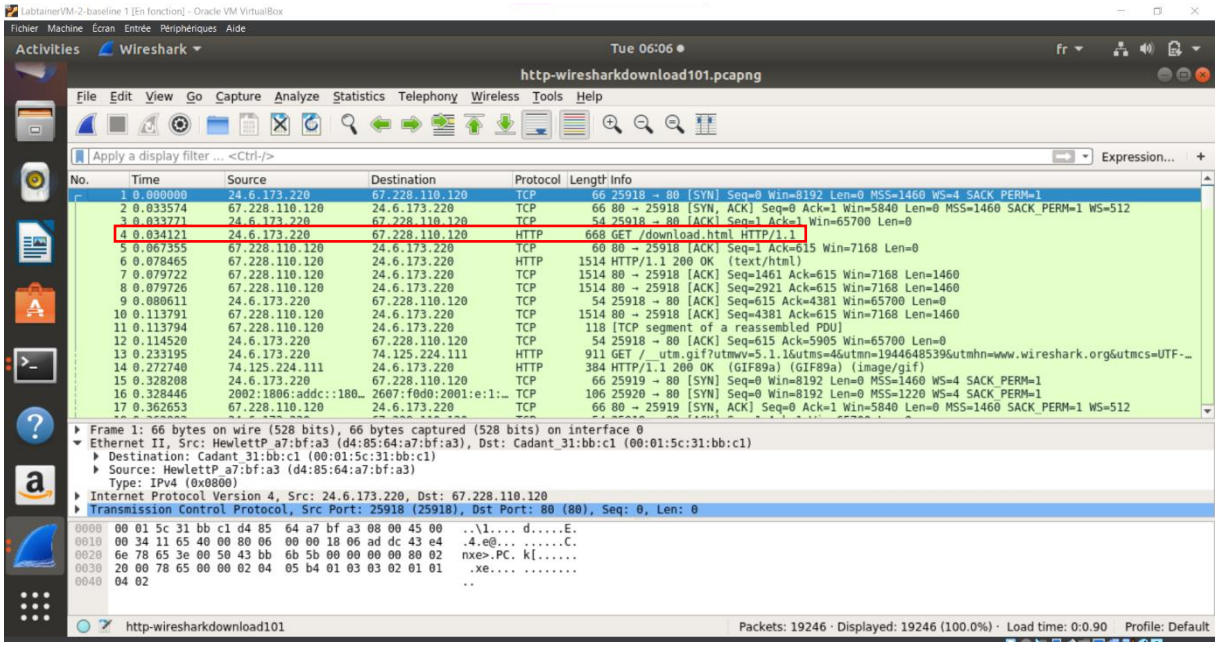


Nous retrouvons bien nos 3 localisations. Et pour chaque adresse, nous retrouvons des informations complémentaires tels que la ville, le nombre de paquets et de bits échangés.

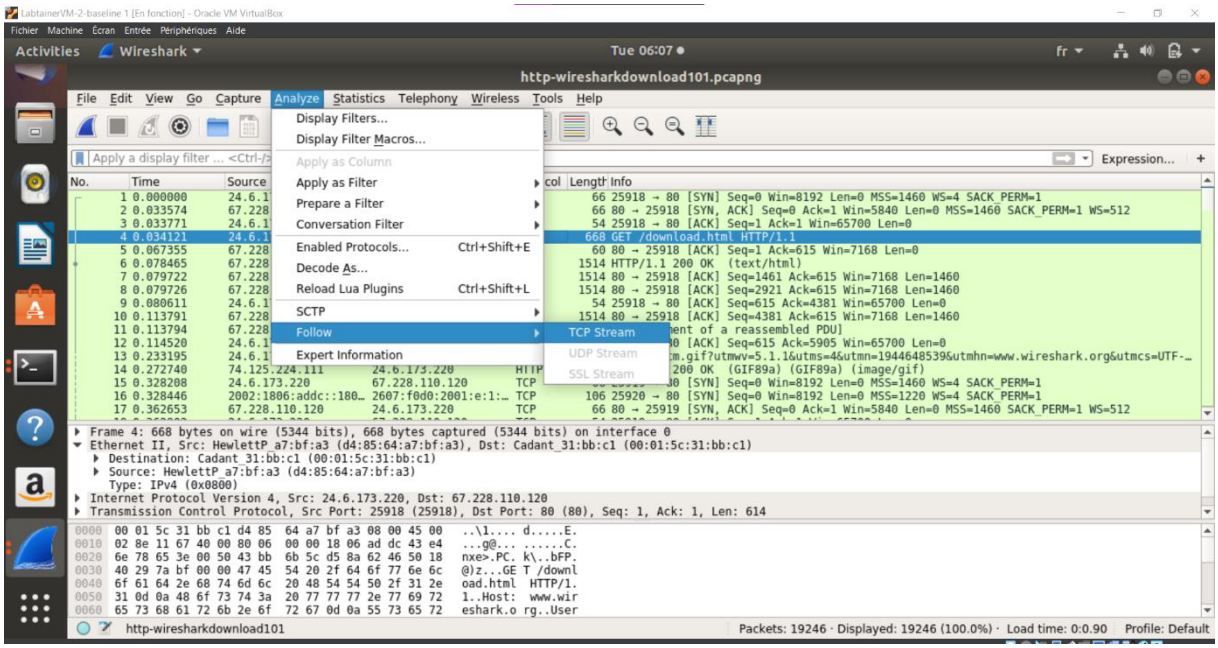
d. Réassembler un texte à partir du flux TCP capturé

Nous allons voir que nous sommes capable de reconstituer un échange entre le client et le serveur.

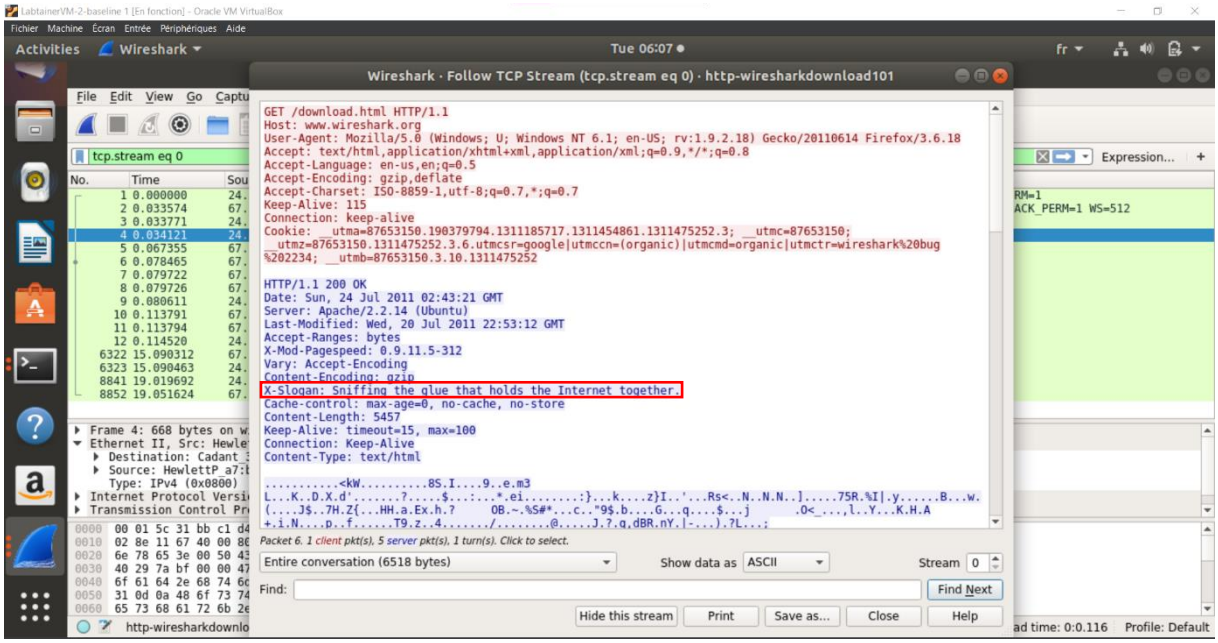
Nous ouvrons maintenant le fichier « pcaps/http-wiresharkdownload101.pcapng ». Nous obtenons les trames suivantes :



Nous observons que la trame 4 est un protocole http utilisant la m méthode get. C'est-à-dire que le client télécharge la page *download.html*. Nous cliquons sur cette trame avec le clic gauche, puis nous sélectionnons l'onglet « Analyze» - « Follow » et « TCP stream ».



Puis nous obtenons la page suivante qui retrace l'échange entre ces deux adresses IP, avec en rouge le client et en bleu le serveur.

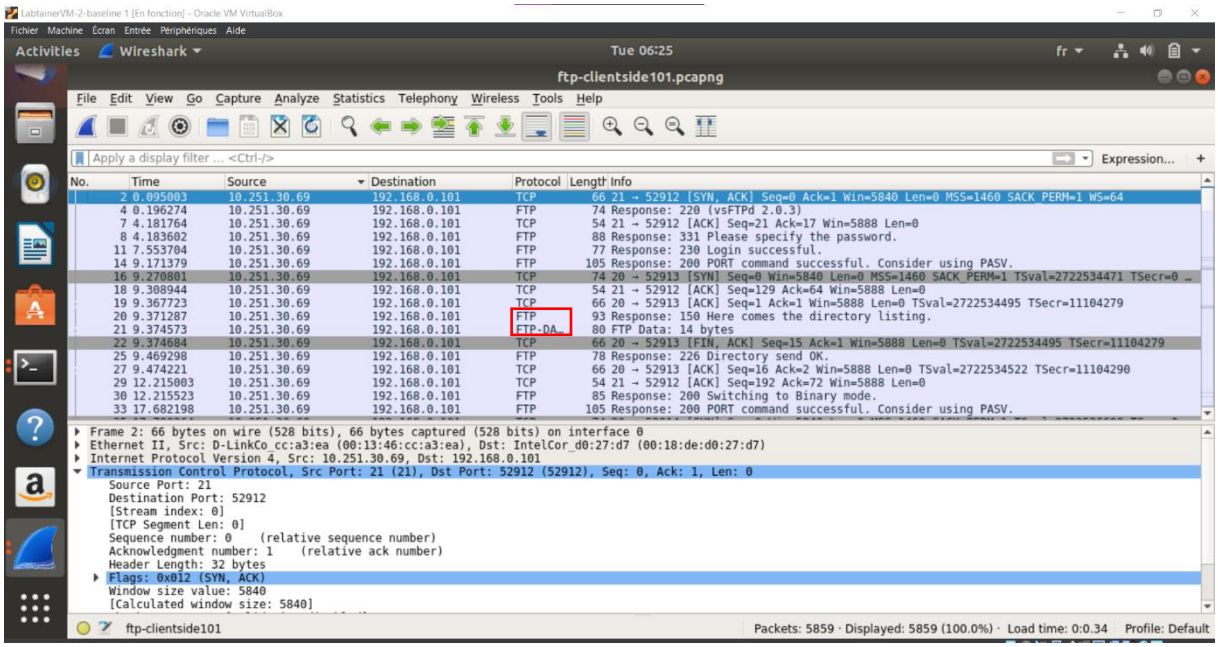


Nous observons qu'un message a été téléchargé : « X-Slogan : Sniffing the glue that holds the Internet together ».

e. Extraire un fichier binaire d'une session FTP

Le protocole FTP qui signifie « File Transfer Protocol » permet de télécharger/envoyer un fichier depuis/à un serveur.

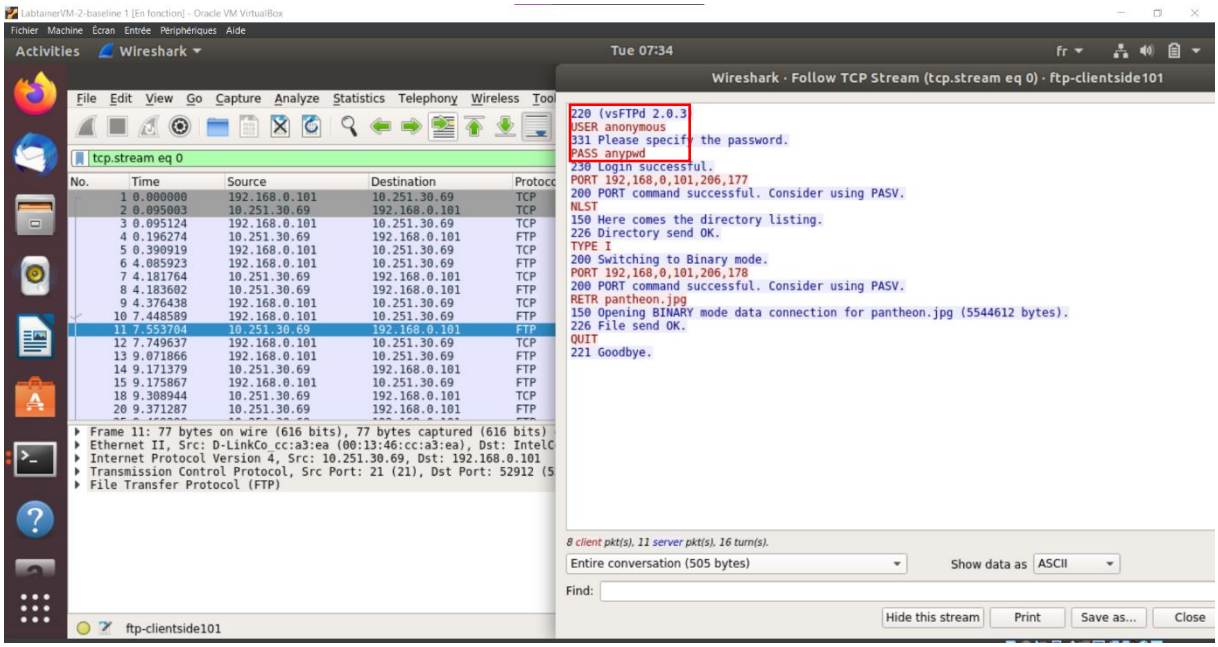
Nous ouvrons le fichier « pcaps/ftp-clientside101.pcapng. Nous obtenons les trames suivantes :



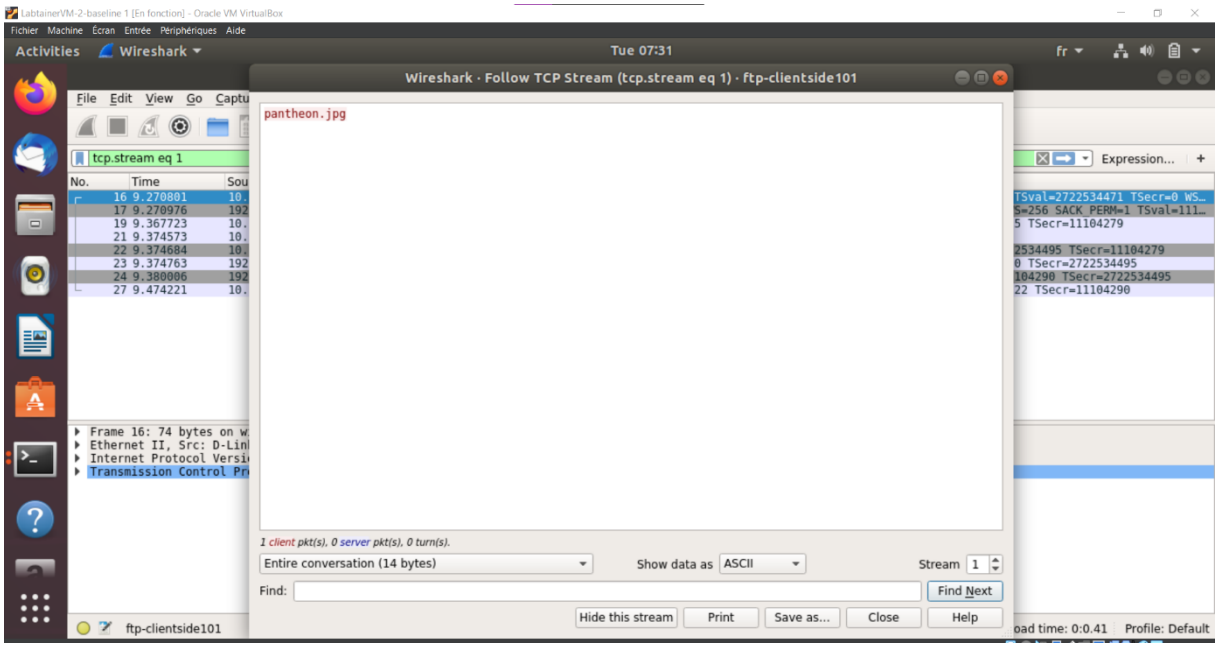
Nous retrouvons deux protocoles :

- FTP : qui permet d'échanger des commandes
- FTP-DATA : qui permet d'échanger des données

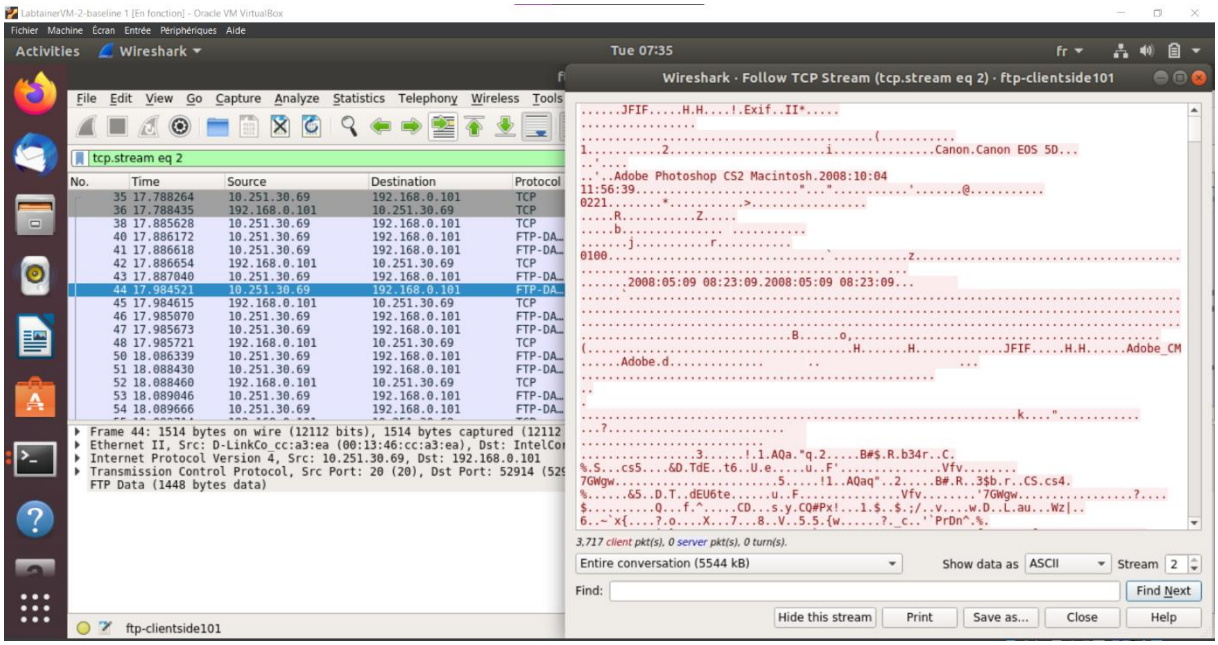
Si nous reconstituons l'échange du protocole FTP, en utilisant la méthode vu dans la partie 4 de ce document, nous obtenons les informations suivantes :



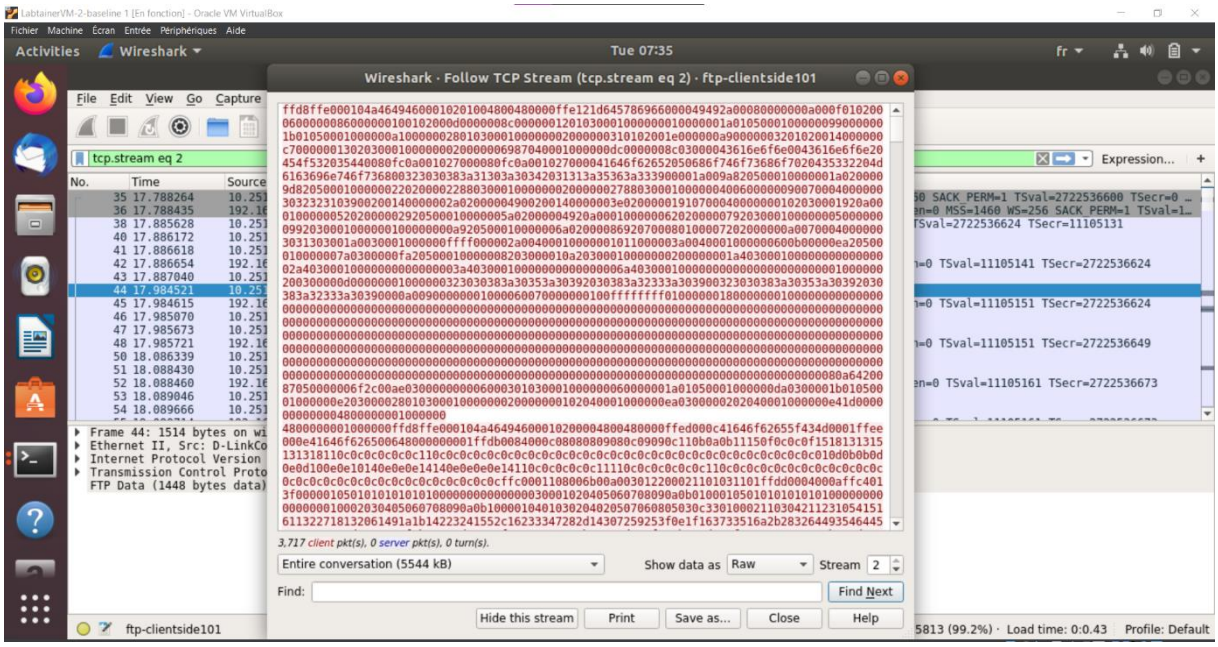
Nous observons que nous retrouvons l'identifiant et le mot de passe pour se connecter au serveur FTP. Maintenant nous retraçons l'échange du protocole TCP.



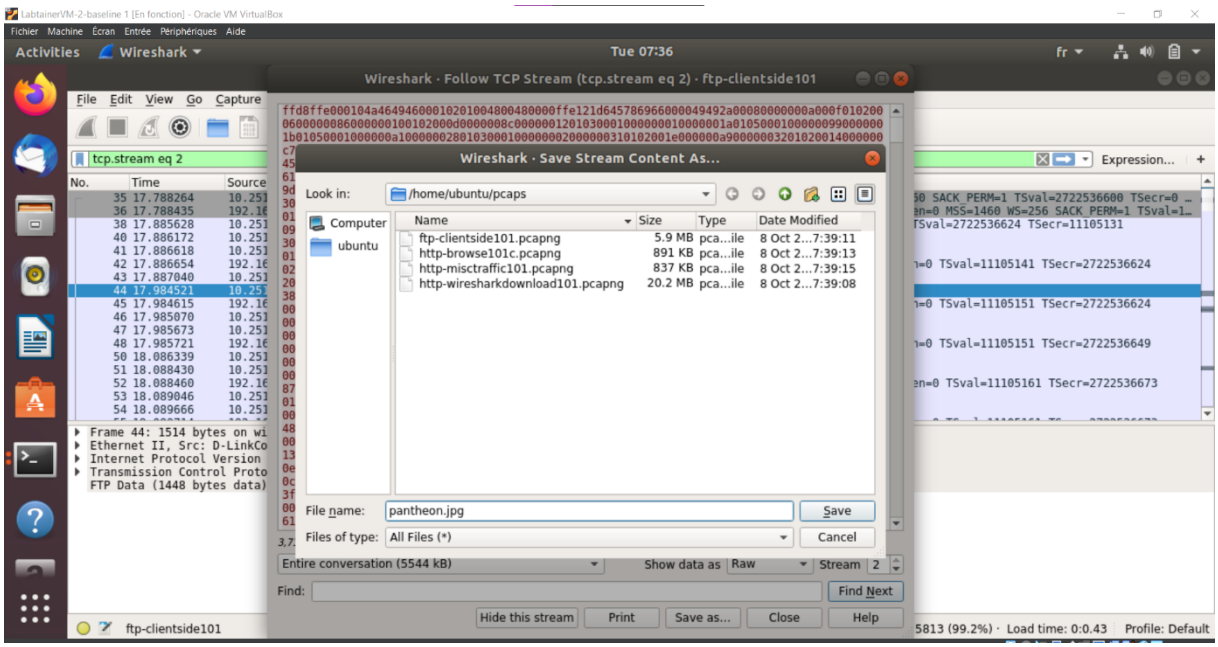
Nous observons le nom du document échangé est « pantheon.jpg ». Nous finissons par retracer l'échange du protocole FTP-DATA.



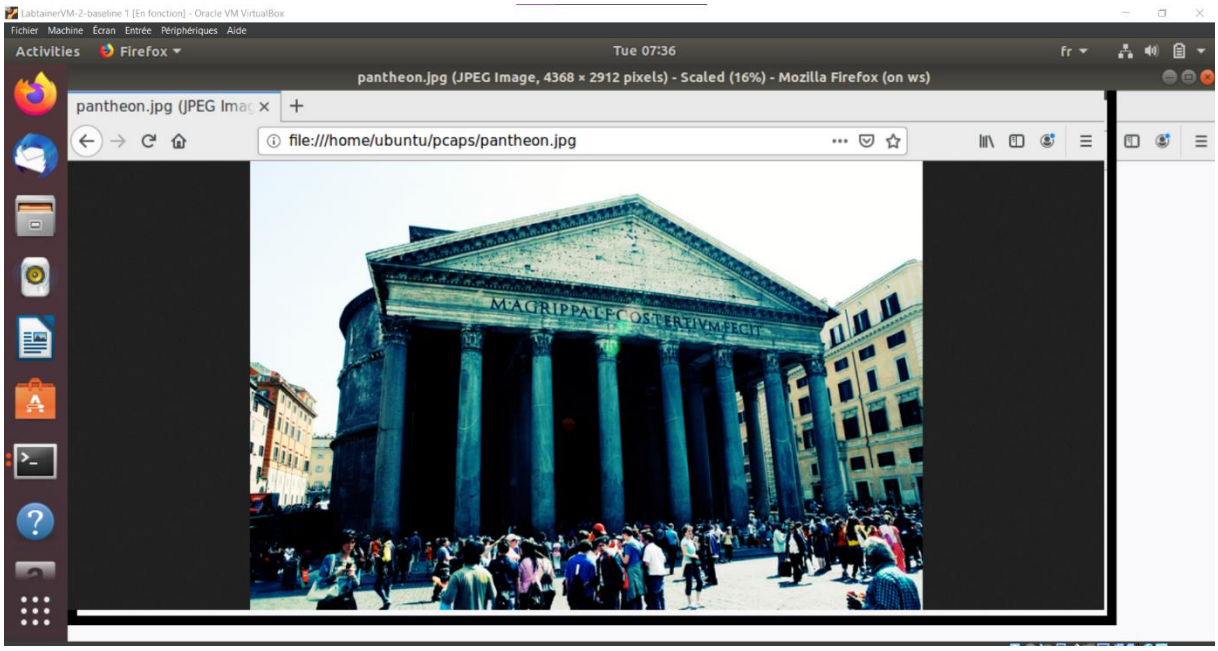
Nous observons que nous retrouvons les données qui correspondent à l'image téléchargée. Nous allons convertir ces données en version .RAW.



Puis nous téléchargeons ce fichier sous le nom « pantheon.jpg ».



Enfin, nous ouvrons firefox, et nous écrivons dans l'URL : http://chemin_du_fichier. Nous obtenons l'image suivante :



4- Conclusion

Par conséquent, nous observons que nous sommes en mesure de rassembler énormément de données à l'aide d'un analyseur de paquets.

Il est néanmoins important de noter que dans ce cas pratique, les protocoles utilisés ne chiffraient pas les données, car nous avons analysé les protocoles HTTP et FTP et non HTTPS et FTPS.